Chief Information Officer's Section
Office of the Governor
State of Utah

December 12, 2001

Network Access Policy

Policy Objectives and Scope: This policy describes the security requirements for connections to State of Utah internal computers and networks. It covers a wide variety of technologies including cellular phone connections, dial-up modem links, value-added networks, and Internet encrypted tunnels (also known as virtual private networks or VPNs). Every employee of the state, citizen acting on private business or internal entity or external entity making these and other types of automated connections to State of Utah internal computers and networks must abide by the rules described here.

Definitions:
Employee: An individual employed by the State of Utah (per *Utah Code Annotated Chapter 67-19-3 et seq*. For purposes of this policy it may include a vendor or contract employee bound by contract to comply with the state security policy.

Citizen: Individual resident of the state or any state acting on personal behalf.

Internal Entity: Any State of Utah department of the executive, legislative or judicial branch, or other office of the state acting for and in behalf of the state as a whole.

External Entity: Any business, non-state governmental agency or office or other organization not described above.

Third Party Connection: Any point at which a Citizen or External Entity establishes a network connection (physical or logical) to the State of Utah Wide Area Network (WAN).

Untrusted Network: Any network where physical and/or logical access and are not subject to monitoring, administration and supervision of the Division of Information Technology Services (ITS). For purposes of this policy this will include Wireless Local Area Networks (any network whose physical medium complies with IEEE 802.11x), any physical connection with an external entity as defined above and encrypted VPN tunnels traversing the state WAN (as well as any other network fitting the definition as untrusted).

Untrusted Network Access Point: the point at which any external entity establishes a *Third Party Connection.* The Division of Information Technology Services will control network access points. The network traffic traversing the Network Access Point will be monitored for known intrusions and other known methods for interfering with normal function of the hosts and network.

Firewall: A method for keeping a network secure from intruders. It can be a single router that filters out unwanted packets or may comprise a combination of routers and servers each performing some type of firewall processing. Firewalls are widely used to give users secure access to the Internet as well as to separate a company's public Web server from its internal network.

External Connections Require Approval: Access to State of Utah internal networks by either state employees or authorized third parties (governmental or non-governmental) from remote locations including worker homes, hotel rooms, customer offices, dedicated line or VPN connection via the Internet, must in all instances be approved in advance by the involved worker's immediate manager as well as the custodian or designate of the information resources to be accessed. Such remote access is not a universal benefit, and may be revoked at any time for cause including unsatisfactory performance and non-compliance with security policies.

Third Party Access to State of Utah Internal Networks: In strictly controlled situations, the State of Utah does allow third parties (defined as vendors, contract personnel and other individuals not fitting the definition of state employee) to access internal networks and connected computer systems. Both the Owner of the information to which the third party will be given access and the project manager in charge of the third party's work must agree in writing to such access before it will be established. The decision-making process for granting such access may include consideration of the controls on the systems to be connected, the third party's security policies, and the results of a background check. Privileges for such third parties must be strictly limited to the system facilities and information clearly needed to achieve predefined business objectives. These access privileges must be reviewed by the relevant project manager to determine whether they need to be continued.

Third Party Vendor Access: Third party vendors, which have sold the State of Utah hardware, software, or communication services, are not automatically granted repeated access to State of Utah internal computers and/or networks. They must either go through the approval process described in the preceding paragraph, or go through a separate remote access for systems maintenance process administered by ITS. Temporary remote access privileges for vendors may, however, be enabled by the systems administrator in charge of the devices or systems without going through either of these approval processes. This temporary access must be granted only for the time period required to accomplish approved tasks (one day or less). This temporary access must be provided by positive identification of the vendor personnel before the connection is established, as well as logging of all activity while the connection exists.

Third Party Compliance Statement: All third parties wishing to remotely access State of Utah internal computers or networks must sign a compliance statement prior to being issued a network user-ID. If a certain third party already has a network user-ID, a signature must be obtained prior to receiving a renewed network user-ID (as indicated above, this renewal process takes place every six months). A signature on this compliance statement indicates the involved user(s) understand and agree to abide by State of Utah policies and procedures related to computers and networks. The State of Utah retains the right to periodically audit third parties who have access to State of Utah computers and networks to ensure compliance with this and other policies and requirements.

Responsibility for User-IDs: All employees and non-employee third parties are responsible for the activity performed with their personal network user-IDs, whether or not these network user-IDs are connecting via external network facilities. Network user-IDs must never be shared with associates, friends, family members, or others. Network user-IDs may not be utilized by anyone but the individuals to whom they have been issued. Similarly, employees are forbidden from performing any activity with network user-IDs belonging to other individuals (excepting anonymous user-IDs like "guest").

Default to Denial: If a State of Utah computer or network access control system is not functioning properly, it must default to denial of privileges to users. If access control systems are malfunctioning, the systems they support must remain unavailable until such time as the problem has been rectified.

Authentication: All computer network connections (for example by dial-up line or the Internet) initiated from a location outside an official State of Utah office, and connecting to a State of Utah internal network, must employ authentication systems consistent with the State Information Security Policy, requiring a minimum of a unique user ID and password.

Outbound Connections: Computer network connections initiated from inside an official State of Utah office, and connecting to an external network or computer, must be routed through dial-up modem pools, Internet firewalls, and other systems expressly established to provide secure network access.

Modems on Desktop Systems: Modems, including fax/modems in or connected to office desktop PCs connecting to a network within the state WAN are not permitted. Home based, mobile and/or telecommuting microcomputers are an exception to this rule. As indicated above, connections to remote computers and networks must instead be routed via modem pools or the State of Utah Internet firewall. Employees with home based, mobile, or telecommuting PCs must not leave modems in auto-answer mode, with communications software enabled, such that incoming dial-up calls could be received.

Encrypted Links: Whenever a computer network connection is established with a State of Utah internal computer or network from a location outside an official State of Utah office, and whenever this connection transmits or is likely to transmit either Confidential or Private information, the link must be encrypted. Such encryption must be accomplished only with systems consistent with standards approved as part of the Utah Technical Architecture, and implemented by agencies and ITS.

Using Radio Technology for Data: Portable phones using radio technology as well as cellular phones must not be used for data transmissions containing State of Utah Private or Confidential information unless the connection is encrypted. Likewise, other broadcast networking technologies, such radio-based local area networks, must not be used for these types of State of Utah information unless the link is encrypted. Such links may be used for electronic mail as long as involved users understand that the transmissions must not contain readable Private or Confidential information. Similarly, employees must not discuss Confidential or Private matters on cordless or cellular phones employing a regular voice connection, unless this connection has been encrypted with technology approved by ITS. Phones using digital transmission rather than traditional analog transmission protocols (such as PCS) are not considered to be encrypted for purposes of this policy.

Privilege Access Controls: All computers permanently or intermittently connected to either external networks or State of Utah networks must operate with privilege access controls recommended by the State Information Security Committee (SISC) and approved by the Information Technology Policy and Strategy Committee (ITPSC). Server systems must employ network user-IDs unique to each user, as well as user privilege restriction mechanisms including directory and file access permissions. Network-connected single-user systems, servers or workstations, must employ approved hardware or software mechanisms that control system booting and that includes a time-out-after-no-activity screen blanker.

Changing Initial Passwords: All vendor-supplied default passwords (or other alternative access mechanisms) must be changed before any computer or communications system is used for any State of Utah business activity. This policy applies to passwords associated with end-user network user-IDs, as well as passwords associated with systems administrator and other privileged network user-IDs.

Shared File Systems: The establishment of a connection between any external computer or network and a State of Utah internal computer or network must not involve the use of shared file systems such as NFS (Network File System). This will help to ensure that sensitive information is not inadvertently disclosed to unauthorized persons. An exception will be made if ITS approves the configuration prior to usage, such as an ad hoc peer-to-peer LAN of devices capable of file and print sharing within a workgroup but not allowing access from the Internet or other untrusted networks.

Required Virus Checking Programs: Up-to-date virus checking programs approved by ITS and/or agency IT security managers must be continuously enabled on all web servers, LAN servers, mail servers, firewalls, and networked PCs. An exception will be made in those cases where the operating system, such as UNIX, is not generally subject to viruses.

Eradicating Viruses: If employees and/or approved, authorized users suspect infection by a computer virus, they must immediately stop using the involved computer and call their agency LAN administrator or Help Desk. Floppy disks and other magnetic storage media used with the infected computer must not be used with any other computer until the virus has been successfully eradicated.

Decompress Before Running Virus Software: All externally supplied computer-readable files (software programs, databases, word processing documents, spreadsheets, etc.) must be decompressed prior to being subjected to an approved virus checking process. Many virus-checking programs cannot detect viruses in compressed files. The same applies to files, which have been encrypted.

Downloading Software: Employees and/or approved, authorized users should not routinely download software from dial-up electronic bulletin board systems, the Internet, or other systems outside the State of Utah. This prohibition is necessary because such software may contain viruses, worms, Trojan horses, and other software, which may damage State of Utah information and systems. An exception is made for systems administrators and other authorized technical personnel downloading patches and the latest releases of software packages. An exception is also provided for external network automated software distribution systems (such as those which distribute the latest virus checking software), which have been approved by agency security managers, and/or ITS.

Time-Out After No Activity: All systems accepting remote connections from public networks such as the dial-up phone network or the Internet must include a time-out system. This time-out system must terminate all sessions, which have had no activity for a period of 30 minutes or less (a smaller time period is recommended). In addition, all user-IDs registered to networks or computers with external access facilities must be automatically suspended after a period of 30 days of inactivity. Agencies with remote offices with infrequent activity may approve exceptions for the convenience of the agency.

Failure to Establish a Connection: All computers with interfaces to external networks must temporarily terminate the connection or time-out the network user-ID for at least ten minutes following a sequence of several unsuccessful attempts to login. For example, if an incorrect dynamic password is provided three consecutive times, dial-up systems should drop the connection. Repeated unsuccessful attempts to remotely establish a connection using a privileged network user-ID must not result in the revocation (suspension as opposed to time-out) of the network user-ID because this could interfere with the ability of authorized parties to respond to security incidents.

Warning Banners: Where systems software permits, login banners must be used on all State of Utah networks and computers, which are directly accessible through external networks. These banners must employ standard no trespassing warning notices adopted by the Information Technology Policy and Strategy Committee (ITPSC). These banners must also refrain from disclosing the fact that State of Utah systems have been reached, the nature of the information available on these systems, as well as the specific systems software running on these systems. Web servers, telephone voice response units (VRUs), and other systems, which are designed to respond to anonymous users, do not need to have such banners.

Anonymous Interaction: With the exception of Web servers, electronic bulletin boards, or other systems where all regular users are anonymous, users are prohibited from logging into any State of Utah system or network anonymously (for example, by using "guest" user-IDs). If users employ systems facilities which allow them to change the active user-ID to gain certain privileges, they must have initially logged-in employing a user-ID that clearly indicates their identity.

Logs for Externally Connected Systems: All State of Utah computers and networks which interface to external networks must maintain system logs which indicate the identity and activity performed by each user who gains access to these systems. These logs must indicate the time of day, the date, the user-ID employed, any special privileges utilized (root, administrator, etc.), and other details associated with all connections (whether permitted or denied). Systems administrators must regularly review these logs or use automated intrusion detection systems to immediately inform them of suspicious activity.

Flow Control for Externally Connected Systems: All State of Utah networks which are connected to external networks must employ flow control to restrict the machines to which users can connect based on the need for such access. Flow control can be implemented via internal firewalls, routers, gateways, VPNs, and other systems. The intention of this flow control is to contain intrusions by unauthorized parties. ITS will control access points for untrusted networks. This policy will restrict the physical and logical connections to centralized entry points to facilitate the monitoring for known intrusions, controlling the flow of network packets, authentication of users and authorization to resources will be managed by the Division.

Browsing: Employees and/or approved, authorized users must not browse through State of Utah computer systems or networks. For example, curious searching for interesting files and/or programs in the directories of other users is prohibited. Steps taken to legitimately locate information needed to perform one's job are not considered browsing. This statement on browsing does not apply to external networks such as the Internet.

Gaining Unauthorized Access: Employees and/or approved, authorized users using State of Utah computer networks are prohibited from gaining unauthorized access to any information system or network to which they have not been expressly granted access. Authorized parties using State of Utah computer networks are also prohibited from in any way damaging, disrupting, or interfering with the operations of information systems to which they are connected. Likewise, employees are prohibited from capturing or otherwise being in possession of passwords, encryption keys, or any other access control mechanism, which has not been expressly assigned to them.

Changes to State of Utah Networks: Changes to State of Utah internal networks include loading new software, changing network addresses, reconfiguring routers, adding dial-up lines, and the like. With the exception of emergency situations, all changes to State of Utah computer networks must be documented in a work order request and must be approved in advance by the agency LAN administrator and/or ITS. Emergency changes to State of Utah networks must only be made by persons who are authorized by ITS. This process prevents unexpected changes from inadvertently leading to denial of service, unauthorized disclosure of information, and other similar problems.

Establishing System Connections: Authorized users must NOT establish or make arrangements for the establishment of electronic bulletin boards, local area networks, modem connections to existing local area networks, or other servers for communicating information without the specific approval of the agency security manager and ITS. Likewise, new types of real-time connections between two or more in-house computer systems must not be established unless such approval has first been obtained from agency IT directors/managers. Provisions will be made to move existing systems into compliance. This policy helps to ensure that all State of Utah systems have the controls needed to protect other network-connected systems. Security requirements for a network-connected system are not just a function of the connected system; they are also a function of all other State of Utah connected systems.

Installation of Communications Lines: Authorized users and vendors must not make arrangements for, or actually complete the installation of voice or data lines with any carrier, if they have not first obtained approval from network planning at ITS.

Subscription to External Networks: Authorized users must not establish connections with Internet Service Providers (ISPs) or other external networks for the transmission of State of Utah data unless this arrangement has first been approved by ITS.

Establishing New Business Networks: Authorized users are prohibited from using the Internet or any other external network to establish new or different business channels. These channels include electronic data interchange (EDI) arrangements, electronic malls with on-line shopping, on-line database services, etc. Exceptions to this rule include planned additions of extranet partners to meet agency specific program requirements, for authentication to public applications and approved transfer of EDI information to qualified vendors.

Participation in External Networks: Participation in external networks as a provider of services that external parties rely on is expressly prohibited unless two conditions are first fulfilled. Specifically, the Division of Risk Management must identify the legal and other risks involved, and then ITS and the agency requesting participation must expressly accept these and other risks associated with the proposal. Acting as an Internet node is an example of such participation. This provision is not intended to interfere with approved external networks currently an integral part of agency business activities.

Disclosure of Systems Information: The internal addresses, configurations, and related system design information for State of Utah computers and networks is confidential and must not be released to third parties who do not have a demonstrable need-to-know such information. Likewise, the security measures employed to protect State of Utah computers and networks is confidential and should be similarly protected.

References:

Organization Sponsoring the Standard: State Information Security Committee (SISC)
State Technical Architect Approval Date: Pending
CIO Approval Date: Pending
ITPSC Presentation Date: Pending
Author(s): Robert Woolley, Rick Gee, Curtis Parker (ITS), SISC
Related Documents: State Information Security Charter, State Information Security Policy, State Acceptable Use Policy, Utah Administrative Rule R365-4 “Information Technology Protection,” State Telecommuting Policy and the Warning Banner Policy.

Appendix A.
Agreement To Comply With Information Security Policies

A signed paper copy of this form must be submitted with all requests for (1) authorization of a new network user-ID, (2) authorization of a change in privileges associated with an existing network user-ID, (3) any periodic reauthorization of an existing network user-ID, or (4) authorizing the connection of an external/untrusted network to the State WAN. Modifications to the terms and conditions of this agreement will not be accepted.

User / Authorized Contact Printed Name: ____________________________________

User Employer / Agency Name: ____

User Telephone Number: ____

User's Office Physical Address: ____

____

____

____

I, the user / agent, agree to take all reasonable precautions to assure that State of Utah internal information, or information which has been entrusted to the State of Utah by third parties (such as clients, or vendors), will not be disclosed to unauthorized persons. At the end of my employment, contract or other association with the State of Utah, I agree to return to The State of Utah all information to which I have had access in order to do my job. I understand that I am not authorized to use this information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal State of Utah manager who is the designated information owner.

I have access to a copy of the State of Utah Information Security Policies, I have read and understand these materials, and I understand how they impact my job. As a condition of continued employment at The State of Utah, I agree to abide by these information security policies. I understand that non-compliance will be cause for disciplinary action up to and including system privilege revocation, dismissal from The State of Utah, as well as criminal or civil penalties.

I agree to choose a difficult-to-guess password as described in the State of Utah Information Security Policies document, I agree not to share this password with others, and I agree not to write the password down unless it has been transformed in an unrecognizable way.

I also agree to promptly report all violations or suspected violations of information security policies to the agency IT manager or security manager and the Division of Information Technology Services security manager.

User Signature: ___________________________________ Date: ______________________